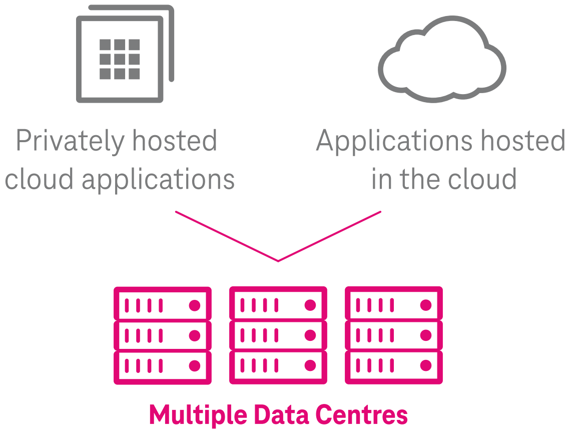
Akamai Edge ServicesLeading Platform for Enterprise Cloud Security Services

Market-leading Cloud Security Services for hybrid & multi-cloud service architectures

The defensible network perimeter no longer exists, at least not in any recognizable form. A security and access approach that made sense 20 years ago is at best misaligned and, at worst, perilous today. Indiscriminate and targeted cyber attacks are rising, and businesses must also manage the risks to their data from insider threats, whether malicious or accidental. The trend towards web-based business processes that aid efficiency and agility introduces new attack surfaces by adding more connections to the Internet and opening new network ports. The combined resources of T-Systems and Akamai position us as leaders in cloud security. Akamai serves up to 30% of the world's web traffic, with extensive insight into market needs. T-Systems' 25-year track record of success in helping organizations throughout their digitalization journey is, in no small part, attributable to our approach to security and strategic alliances. We wrap our cloud ecosystems and solutions in services designed to protect your data and users 24/7/365.


Privately hosted cloud applications
Applications hosted in the cloud
Multiple Data Centres

Employee challenges

- Secure application access
- Acceptable use policy enforcemen

Application protection

- Denial of service
- Web application firewall
- Bot management
- DNS services

Infrastructure services

- Denial of service
- Malware prevention
- Micro-segmentation for zero-trust security

Why choose us for your cloud security services?

All security services are provided through Akamai's global edge services platform, which serves over a quarter of all internet traffic. It is the foundation for threat intelligence solutions that make security more effective and easier:

- The latest DDoS attack vectors are immediately visible and investigated by Akamai, often before anyone else. To mitigate them, Akamai rapidly implements new security measures. For example, it discovers different types of web application assaults and updates automated rules that can also protect against new vulnerabilities.
- Bots are characterized and studied as they develop and interact with client organizations' websites, enabling individual management of each bot.
- Reputation services have total visibility of previous malicious actions detected, which allows for more informed security choices.
- The SOC's newly acquired intelligence aids in the detection of unauthorized attempts to access sites from within a network, ensuring prompt responses.

Our solutions at a glance

Prolexic DDoS protection services – Volumetric attacks against infrastructure services

Over 20 globally deployed carrier-independent scrubbing centers provide the biggest bandwidth and highest SLAs. Always-on DDoS security services.

Application & API Protector – WAF services at their best

Full-blown features and functions set, which is recognized by Gartner as market-leading. Integrated learning capabilities provide automated update management to minimize operational efforts and maintain up-to-date security policies.

Edge DNS – 100 % available DNS Services

A separated DNS service platform, the cloud-based solution increases the availability, performance, and resilience of DNS resolution. It also improves the user experience for web services. Deployed in private data centers or public clouds and complements existing web infrastructures.

Bot Management – Know the Bots accessing your infrastructure

Bot management with identification, categorization, management, and visibility into bot traffic. It helps report the bot traffic to effectively manage the business and IT impact of bots. Capable of catching the most sophisticated bots for web fraud like credential abuse and gift card balance checking.

Enterprise Application Access – Zero Trust Access

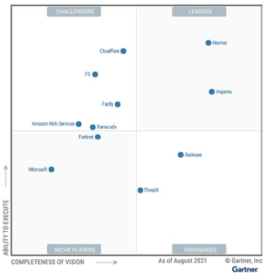
A cloud-delivered, identity-aware, high-performance service provides secure application access for users whenever and wherever they need it. It avoids network connectivity and is available for all web services, including clientless and client-based.

Enterprise Threat Management – Secure your infrastructure services

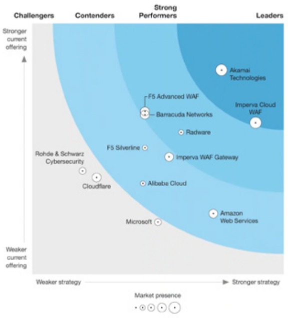
A proven, globally distributed DNS platform leverages real-time cloud security intelligence. Proactive and rule-based, it identifies and blocks targeted threats, like malware, ransomware, DNS data exfiltration, and phishing. Centrally managed and enforced unified security and acceptable use policies in minutes for all employees.

Guardicore Micro-Segmentation Services – Prevent ransomware attacks

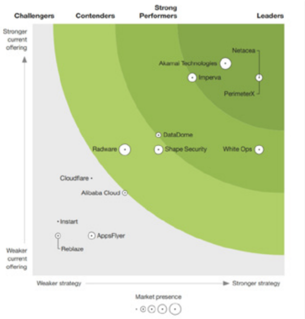
Improves security without downtime by breaking down the network into specific software-based segments and enhancing their defenses faster and simply. The policy engine enables complete insight into the IT environment and self-defense system. Allows the creation of granular security policies with accuracy and certainty.



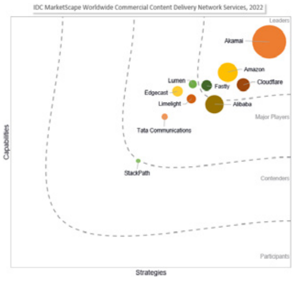
Gartner Magic Quadrant
für Web Application &
API Protection 09/2022



Forrester WaveWeb
Application Firewall,
Q1 2020



Forrester Wave
Bot-Management,
Q1 2020



IDC Worldwide
Commercial CDN
08/2019

DO YOU HAVE QUESTIONS?
0800 33 09030

VISIT US:
www.t-systems.com/de/de

PUBLISHER
T-Systems International GmbH
Hahnstraße 43d
60528 Frankfurt am Main
Germany

T Systems Let's power
higher performance